

# NIAC Working Group on Cross Sector Interdependencies & Risk Assessment Guidance

---

## Proposed Transmittal Letter

Martin G. McGuinn, Chairman & CEO  
Mellon Financial Corporation

Tuesday – January 13, 2004

# Presentation Outline

---

- ❑ Background
- ❑ Report on Actions to Date
- ❑ DHS Briefings
- ❑ Key Issues and Proposed Recommendations
- ❑ Fundamental Principles
- ❑ Appendices

# Background

---

- April 22 – NIAC Members recommend establishment of working group to:
  - Provide risk assessment guidance based on cross-sector interdependencies and gaps identified in the process.
  - Provide advice and guidance to the President on what needs to be addressed.

# Report on Actions Taken to Date

---

<input type="checkbox"/> Project Initiation	May 8, 2003
<input type="checkbox"/> Kick-off Meeting	May 14, 2003
<input type="checkbox"/> Progress Report	July 22, 2003
<input type="checkbox"/> Recommendations Presented	Oct. 14, 2003
<input type="checkbox"/> NIAC members review	
<input type="checkbox"/> DHS updates provided	Dec. 1, 2003
<input type="checkbox"/> HSPD 7 & 8 issued	Dec. 18, 2003
<input type="checkbox"/> DHS reviews HSPD 7	Dec. 19, 2003
<input type="checkbox"/> Draft Transmittal Letter	Dec. 24, 2003

# DHS Briefings

---

- Briefing on role of Infrastructure Coordination Division – December 1
  - Coordinates with and across sectors
- Briefing on new Homeland Security Presidential Directive 7
  - HSPD 7 - Critical infrastructure identification, Prioritization and Protection
  - HSPD 8 – National Preparedness

# Key Policy Recommendations:

---

- ☐ Formalize the Public/Private Partnership
- ☐ Prioritize Federal Critical Mitigation Activities

# Formalize the Public/Private Partnership

---

- Formalize a framework for including private sector in all phases of developing, implementing, and sustaining processes designed to protect
  - Private sector wants to insure the security and resiliency of its strategic assets
  - Private sector needs to be an integral part of the planning process
  - Federal government needs to provide the structure by which private sector can interact – before, during and after an emergency

# The National Incident Management System (NIMS) can provide a framework for public-private critical infrastructure incident management and emergency response.

---

- ❑ HSPD – 5 directed DHS to develop and administer NIMS. NIMS provides a consistent approach for all levels of governments to prepare for, respond to, and recover from domestic incidents.
- ❑ The directive also required development of a National Response Plan. This plan, using NIMS, provides the mechanism for national-level policy and operational direction for Federal support to State, tribal, and local incident managers and for exercising direct Federal authorities and responsibilities.
- ❑ All Federal departments and agencies are required to adopt NIMS. Adoption by State and local organizations is a requirement for Federal preparedness assistance.
- ❑ The current NIMS draft should be revised to include a critical infrastructure role for the private sector to ensure a coordinated and effective approach to emergency planning and crisis response at all levels.



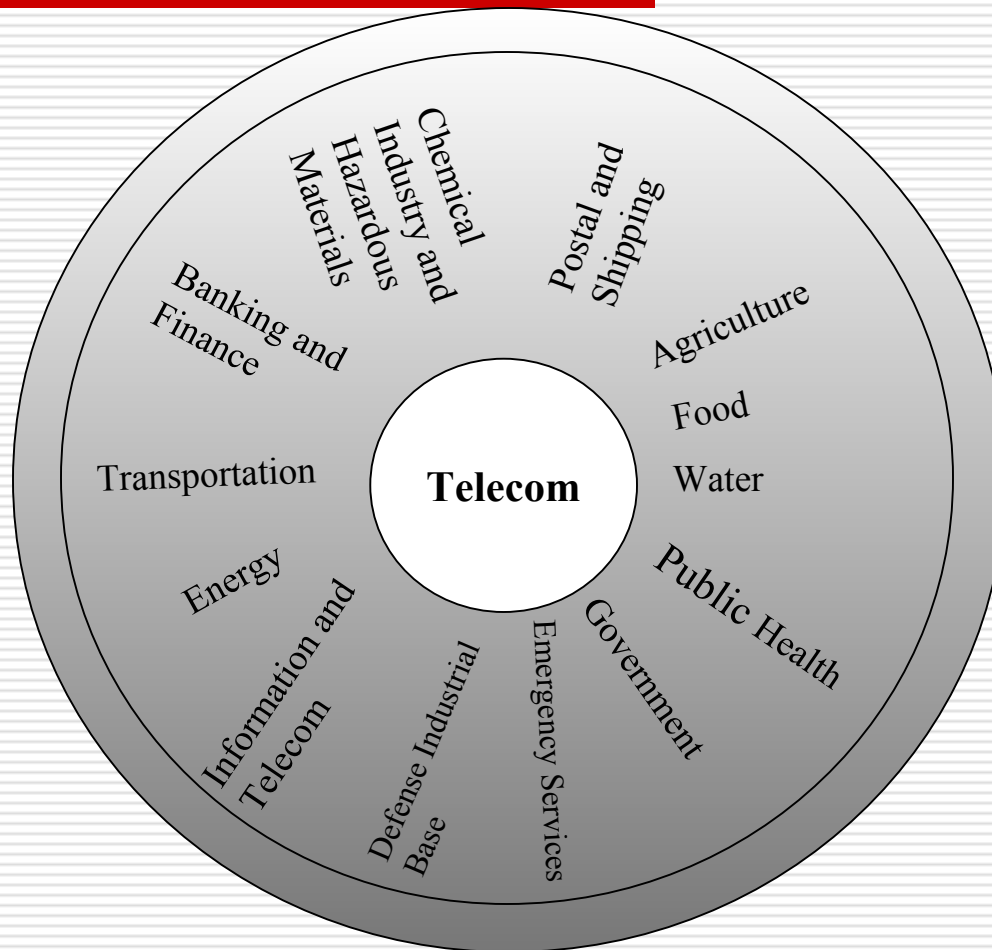
# Prioritize Federal Critical Mitigation Activities

---

- Concentrate Federal efforts on those industries on which we are most reliant:
  - Nearly universal dependence on telecommunications to operate other infrastructure components.
  - Energy is necessary for facilities and equipment used in telecommunications to operate.

Telecommunications represents a “base” infrastructure on which all other sectors depend.

---



---

*Source: Based on concept designed by Steve Malphrus and Angela Desmond, Federal Reserve Board*

# Fundamental Principles

---

- ❑ Projects must be structured to provide short-term deliverables to address the most pressing issues in a useful, if non-optimal, fashion.
- ❑ Progress must be monitored to ensure adequate progress is made toward implementing approved recommendations.
- ❑ Partnership between the public and private sectors must be a two-way street in order to evolve to a “trusted” partnership.

# Appendices

---

- ❑ Cross Sector Interdependencies and Risk Assessment Guidance
  - October 14 Proposed Recommendations
  - Relevant portions of Homeland Security Presidential Directives 7 and 8
- ❑ Working Group Participants
- ❑ Deliverables Contained in Report of Proposed Recommendations

1. Inconsistencies exist in the definition of the critical infrastructures.
- 

- Promote organizational consistency using the definitions for Critical Infrastructures contained in the National Strategy for Homeland Security.
- HSPD 7 - Section 6a
  - The term critical infrastructure has the meaning given to that term in the USA Patriot Act , and referenced in the National Strategy for Homeland Security.

## 2. The sector coordinator role is not broadly understood by private industry.

---

- ❑ We support the concept of sector coordination – participating in, coordinating, and supporting private/public and cross sector collaborative efforts.
- ❑ Coordinator role should be defined and publicized to the CEOs, CIOs, and crisis managers of their sectors.
- ❑ HSPD 7 – Section 14
  - Establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors, along with metrics and criteria for related programs and activities.

3. Crisis Management plans do not exist for each sector and are not tested end-to-end, across the sectors.

---

- ❑ Crisis Management Plans should exist for each sector and be tested.
- ❑ Testing should include cross-sector coordination.
- ❑ Testing and exercising sector crisis management plans should be under the purview of the sector coordinator.
- ❑ HSPD 7 – Section 19
  - Sector-Specific agencies shall conduct vulnerability assessments of the sector, and encourage risk management strategies to mitigate the effects of attacks against critical infrastructure and key resources.

4. A National Command Center does not exist as a confluence point for the private sectors during times of crisis.

---

- ❑ DHS should establish a virtual command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency situation.
- ❑ Each sector should have a seat at the Homeland Security Operations Center.
- ❑ Homeland Security Act of 2000
  - Homeland Security Operations Center (for DHS) and the National Incident Command Center (for IAIP) will provide.



5. Government sponsored exercises (e.g., TOPOFF2) do not actively solicit private industry representation.

---

- ❑ DHS should sponsor crisis management exercises that include the participation of the critical infrastructures as soon as possible, and annually thereafter.
- ❑ Lessons learned from such exercises should be made available as appropriate and provided to the private sector.
- ❑ HSPD 8 – Section 18
  - Establish a national program to conduct homeland security related preparedness exercises.
  - Develop a system to maintain and disseminate lessons learned, best practices and information from exercises, training events, research and other sources.

## 6. There is an underestimation of the dependency of the Nation's critical infrastructures on the Internet.

---

- ☐ Support initiatives to enhance awareness of Internet dependencies, by encouraging the:
  - Private industry to:
    - ☐ Adopt security practices
    - ☐ Encourage users to keep skills and knowledge current
    - ☐ Help educate users
  - Technology Vendors to:
    - ☐ Design virus resistant-virus proof software
    - ☐ Reduce implementation errors
    - ☐ Ship products with high-security default configurations
  - Government to:
    - ☐ Provide incentives for higher quality software
    - ☐ Support a research agenda that seeks new approaches to software security
    - ☐ Encourage more technical specialists
    - ☐ Provide more awareness and training for internet users
- ☐ HSPD 7 – Section 22c

7. Coordination in planning and response between public emergency management and private critical infrastructure is inadequate and/or inconsistent.
- 

- ❑ Provide a framework for public and private emergency management interaction at the national, sector, state, and regional levels. The framework should integrate with public and private information sharing models and account for Information Sharing and Analysis Centers and InfraGard.
- ❑ HSPD 7 – Section 27
  - Produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources, including a strategy to identify, prioritize and coordinate the protection of critical infrastructure and key resources, including how the government intends to work with Federal departments and agencies, state and local governments, the private sector, and foreign countries and international organizations.

8. There is a lack of incentives that would help defray the expense burden resulting from strengthening the resiliency of the critical infrastructures.
- 

- Consider forming a working group to explore the potential for creating tax incentives or other instruments to incent the private sector to enhance the resiliency of the critical infrastructures.
- HSPD 8 – Section 8 – 13
  - The primary mechanism for delivery of Federal preparedness assistance will be awards to the states.
  - There may be activity going on in DHS; should be synchronized with any other efforts underway.

9. Sophisticated modeling capabilities exist at the national laboratories and multiple research and development studies on cross-sector interdependencies have been completed.
- 

- The national labs should focus their interdependency modeling and research on the regions and sectors whose failure would have the greatest impact on the economy and national security.
  - The working group suggests modeling the telecommunications and energy sectors, and the interdependencies among them and the other critical infrastructures.
  - Existing research and development studies should be indexed and cross-referenced in such a way to make these materials accessible to appropriate parties.
  - HSPD 7 – Section 32
    - Use existing and develop new capabilities as needed to model comprehensively the potential implications of terrorists exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate to develop appropriate mechanisms.
-

# Appendices

---

- ☐ Working Group Participants
- ☐ Deliverables Contained in Report of Proposed Recommendations

# Working Group Participants

---

## □ NIAC Member Institutions and DHS Support

- Susan Vismor, SVP, Mellon Financial Corp., Working Group Chair
- Teresa C. Lindsey, Chief of Staff, BITS
- Peter Allor - ISS
- Bob Bergman, UPS
- Andy Ellis - Akamai
- Bobby Gilham - Conoco Phillips (Also listed as sector coordinator)
- Rick Holmes - Union Pacific Corp.
- Douglas Hurt - V-One
- Aaron Meckler - Wells Fargo & Company
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Nancy Wong, DHS
- Eric Werner, DHS
- Clay Woody, DHS

# Working Group Participants

---

## □ Sector Coordinators

- Kathryn Condello, CTIA, Telecommunications \*
- Matthew Flanigan, TIA, Telecommunications\*
  - Dan Bart, TIA
  - David Thompson, TIA
- Michehl Gent, North American Electric Reliability Council, Electric Power \*
  - Lou Leffler, NERC
  - Dave Nevius, NERC
- Bobby Gillham, ConocoPhillips, Inc., Oil and Gas \*
- Ed Hamberger, Association of American Railroads, Surface Transportation\*
  - Nancy Wilson, Association of American Railroads
- Rhonda MacLean, Bank of America, Financial Services \*
  - Peggy Lipps, Bank of America
- Harris Miller, ITAA, Information\*
  - Greg Garcia, ITAA
- Daniel Phythyon, USTA, Telecommunications\*
  - David Kanupke, USTA
- Diane Van DeHei, Association of Metropolitan Water Agencies, Water \*
- Tim Zoph, Northwestern Memorial Hospital, Healthcare

---

\* *Accepted to participate to date (or send substitute).*



# Deliverables

---

- ❑ Critical Infrastructures
  - Critical Infrastructures and Federal Liaison Organizations
  - Matrix of Roles Related to Critical Infrastructure Protection
  - Status of Current Information Sharing and Analysis Centers
- ❑ Sector Coordinators
  - Roles and Responsibilities Definition
- ❑ Crisis Management Coordination
  - Sector Call Trees
  - Sector Approaches to Security/Crisis Management
    - ❑ Railroad, Electricity, and Financial Services Sectors
- ❑ National Command Center Presentation Overview
- ❑ Government Sponsored Exercises
  - Blue Cascades' Key Findings

# Deliverables (*continued*)

---

- ❑ Dependency on the Internet
  - Business Impact Survey Questions
  - Excerpts from Testimony of Richard D. Pethia, CERT
- ❑ Coordination in Planning
  - Business Incident Coordination System (Example)
  - National Crisis Management Partnership (Example)
- ❑ Lack of Incentives
  - Recommendation for a Future Working Group Study
- ❑ Research and Development and Modeling Capabilities
  - Matrix and abstracts of Reports on Critical Infrastructure Interdependencies
  - Ranking of Interdependencies by Critical Infrastructure Sector Representatives